VII

Commission Recommendations

A. Recommendations Regarding the IRSG Principles

- **The Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles.**

The present challenge is to protect consumers from threats to their psychological, financial, and physical well-being while preserving the free flow of truthful information and other important benefits of individual reference services. The Commission commends the initiative and concern on the part of the industry members who drafted and agreed to the IRSG Principles, an innovative and far-reaching self-regulatory program. The Principles address most concerns associated with the increased availability of non-public information through individual reference services. With the promising compliance assurance program, the Principles should substantially lessen the risk that information made available through the services is misused, and should address consumers' concerns about the privacy of non-public information in the services' databases. Therefore, the Commission recommends that the IRSG Group be given the opportunity to demonstrate the viability of the IRSG Principles. *(For a detailed analysis of the IRSG Principles, see Section VI, supra.)*

- **The Commission looks to industry members to determine whether errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls.**

While the Commission believes the IRSG Principles address most areas of concern, certain issues remain unresolved.[303] Most notably, the Principles fail to provide individuals with a means to access the public records and other publicly available information that individual reference services maintain about them. Thus, individuals cannot determine whether their records reflect inaccuracies caused during the transmission, transcription, or compilation of such information. The Commission believes that this shortcoming may be significant, yet recognizes that the precise extent of these types of inaccuracies and associated harm has not been established. An objective analysis could help resolve this issue. The IRSG Group has acknowledged the Commission's position, and has demonstrated its awareness of this problem

by (1) stating that it will seriously consider conducting a study of this issue and (2) agreeing to revisit the issue in eighteen months. The Commission looks to industry members to undertake the necessary measures to establish whether inaccuracies and associated harm resulting from errors in the transmission, transcription, or compilation of public records and other publicly available information are sufficiently infrequent as to warrant no further controls. *(For a detailed discussion of this issue, see Sections IV(B), V(C), supra.)*

B. Recommendations Regarding the Industry Generally

The Commission acknowledges that not every concern associated with the look-up services industry can be resolved by the individual reference services themselves. Rather, certain issues are within the control only of primary sources of information, other information providers, or of users of the information. Thus, understandably, the Principles cannot and do not address every concern associated with the industry. The Commission's recommendations with regard to concerns that cannot be addressed through the Principles are set forth below.

- **The Commission encourages public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices.**

The Commission has found that the easy availability of sensitive, unique identifiers (*e.g.*, Social Security number, mother's maiden name, and date of birth) listed on public records increases the risk of serious harm. Given that information about such risks has surfaced only recently, public agencies may not have yet considered these risks in formulating their public records collection and dissemination practices. Thus, it is possible that certain government agencies may require and/or make available unique personal identifiers even though the collection and dissemination of that information is not essential to advance that agency's intended purpose. The Commission encourages public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. *(For a detailed discussion of this issue, see Sections II(2)(B)(1), IV(C), V(A)(2), supra.)*

- **The Commission urges online white-pages directory services that have not yet done so to implement important privacy safeguards, including not publishing unlisted directory information and allowing individuals to opt out of their databases.**

The Commission commends those online white-pages directory services that have voluntarily addressed consumer privacy concerns by allowing individuals to opt out of their database and by not publishing unlisted directory information. The Commission urges online white-pages directory services that have not yet done so to implement important privacy safeguards. *(For a detailed discussion of this issue, see Sections II(D), VI at 25, supra.)*

- **The Commission encourages users of individual reference services, where not otherwise required by law, to notify individuals voluntarily of adverse decisions based on information obtained through an individual reference service, and to disclose the source of such information, provided such disclosure would not hinder law enforcement or fraud prevention.**

The Commission has learned that users of look-up services may erroneously make adverse decisions affecting individuals because of inaccurate information obtained from individual reference services. Often, such individuals would have no way of knowing that information about them had been obtained, that it was inaccurate, or that it formed the basis for an adverse decision.[304] With adequate notification, such individuals could determine whether inaccurate information about them was disseminated, and, if appropriate, they could attempt to correct it. Accordingly, the Commission encourages users of individual reference services, where not otherwise required by law, to notify an individual voluntarily when they have made an adverse decision about that individual based on information obtained through an individual reference service. This voluntary adverse action notice should also disclose the source of the information on which the decision is based, provided such disclosure would not hinder law enforcement or fraud prevention. *(For a detailed discussion of this issue, see Section IV(B), supra.)*

- **The Commission recommends continued and enhanced consumer and business education.**

Finally, the Commission acknowledges the meaningful efforts undertaken by many privacy advocates, consumer groups, government agencies, and industry members to educate consumers and businesses about information privacy issues. The Commission looks forward to working with all of these groups to better inform consumers and businesses.

Endnotes

1 In June of 1996, LEXIS-NEXIS released a locator product for its subscribers called P-Trak, and marketed the product's ability to find an individual's name, aliases, current and prior addresses, month and year of birth, and Social Security number. Roughly one week later, after a deluge of telephone calls from subscribers, the company provided individuals with the ability to have their information suppressed from the database ("opt out") and discontinued displaying Social Security numbers. Subscribers could still use a Social Security as a search term, to retrieve an individual's name and address. The following September, a message about P-Trak was posted to RISKS, an Internet discussion group that focuses on the risks of computer technology. Word of P-Trak then spread across the Internet and LEXIS-NEXIS was soon flooded with thousands of phone calls protesting, *inter alia,* the accessibility of Social Security numbers from the database. Stories about P-Trak and the public outcry appeared in both the *Washington Post* and the *Wall Street Journal. See* Mary J. Culnan, "Self-Regulation on the Electronic Frontier: Implications for Public Policy" in *Privacy and Self-Regulation in the Information Age*, US Dept. of Commerce, NTIA, June, 1997 at 50-51.

2 The senators requested that the study encompass the collection, compilation, sale, and use of computerized databases that contain consumers' identifying information, without their knowledge. *See* Letter from Senators Larry Pressler, Richard H. Bryan, and Ernest F. Hollings to Commission (October 8, 1996). Separately, Congress requested the Board of Governors of the Federal Reserve System ("FRB") to conduct a study concerning the availability to the public of sensitive information about consumers, whether such information could be used to commit financial fraud, and if so whether its availability caused an undue potential risk of loss for depository institutions. 61 *Federal Register* 68,044 (December 26, 1996). The FRB released its report in March. Federal Reserve Board, Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud, March 1997 [hereinafter "FRB Report"].

3 The study was announced in the *Federal Register* last March. 62 *Federal Register* 10,271 (March 6, 1997). The Commission undertook this examination pursuant to Section 6 of the FTC Act, 15 U.S.C. § 46 (1997). In particular, Section 6(a) authorizes the Commission to "gather and compile information concerning . . . any person, partnership, or corporation engaged in or whose business affects commerce . . . ." *Id.* at § 46(a). Section 6(f) permits the Commission "to make annual and special reports to the Congress . . . ." *Id.* at § 46(f).

4 *See* letter from Commission to Senator John McCain (February 28, 1997). In general, the FCRA (15 U.S.C. §§ 1681-1681u (1997)) governs the sale of consumer credit and other data compiled by agencies such as credit bureaus to parties evaluating individuals for credit, insurance, employment, or similar purposes. As set forth in detail below, many individual reference services offer a broad range of information, from purely identifying data, the primary focus of the study, to a vast array of other data gleaned from public records and other sources. Customers of the services use such information for locating individuals and verifying identities, as well as for many other purposes.

5 Appendix A describes the Commission's information-gathering efforts in connection with the study.

6 Other types of personal identifying information are described more fully in Section II.B. *infra.*

7 *See* H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America.* Univ. Press 1994, at 9, 178-79, 181-83. *See also,* United States Government, National Information Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure*, Draft for Public Comment (1997) at 1, 6; Carole Lane, *Naked in Cyberspace*, Pemberton Press 1997 at 44; Transcript of FTC Consumer Information Privacy

Workshop, June 10, 1997 [hereinafter "Transcript"], Cerasale at 93-94; Varney at 95-96; Wenger at 102; Rotenberg at 104; Baity at 157-58. Unless otherwise indicated, footnote citations are either to the printed transcript of the June 10, 1997 Workshop or to public comments submitted pursuant to the March 6, 1997 *Federal Register* notice [hereinafter Comment, __ (Doc. No. __)]. The Workshop agenda can be found at Appendix B. A list of comments can be found at Appendix C. All of these materials are on file at the Federal Trade Commission's Public Reference Room, File No. P974806, and are available online at *Federal Trade Commission, Consumer Information Privacy Workshop* (last updated December 5, 1997) 7 <http://www.ftc.gov/bcp/privacy2>.

8 Smith, *supra* n. 7, at 181-83; *see also* Transcript, Hendricks at 83-84.

9 Smith, *supra* n. 7, at 7; Lane, *supra* n. 7, at 44.

10 Smith, *supra* n. 7, at 7-9; Transcript, Dick at 78; Lane, *supra* n. 7, at 45.

11 Smith, *supra* n. 7, at 178-79.

12 Smith, *supra* n. 7, at 178-79.

13 *Id.* at 8; Lane, *supra* n. 7, at 44. Today in the United States, 40 million computer information terminals sit on consumers' desks. Transcript, Dick at 126.

14 Louis Harris & Associates and A. Westin, *Commerce, Communication, and Privacy Online, Report on National Survey of Computer Users*, 1997 [hereinafter "1997 Harris Survey"] at 1; Lane, *supra* n. 7, at 22.

15 *See* Naom, *Privacy and Self-Regulation: Markets for Electronic Privacy* at n. 33 in *Privacy and Self-Regulation in the Information Age* (published by Dept. of Commerce, NTIA) 1997; *USA Today* Editorial "But this Nut's Tougher" 10/24/95. Eight companies report that together they employ over 5,000 employees to administer their individual reference services. Comments of Individual Reference Services ("IRSG") at 2 (Doc. No. 35). The whole information industry is growing rapidly. For example, in 1994, revenues from business information services exceeded $28 billion and, for the five years prior, the market for those services grew 6% annually. Comments of Information Industry Association ("IIA") at 6 (Doc. No. 32) (citing Veronis Suhler & Associates, *Communications Industry Forecasts*, 296, 305, 309 (9th ed. 1995)). The investigations industry, alone, has projected revenue to reach $4.6 billion by the year 2000 (four times the revenues in 1980). N. Bernstein, "Electronic Eyes: What the Computer Knows -- A Special Report; On Line, High-Tech Sleuths Find Private Facts," *New York Times*, September 15, 1997 at 1.

16 *See* discussion of online reference services at Section II.D. *infra.*

17 In fact, apparently in response to this study, commercial entities that provide, directly or as suppliers to others, individual reference services, defined themselves as the individual reference service industry. *See* Comments of IRSG at 2 (Doc. No. 35); CDB Infotek at 5 (Doc. No. 20).

18 In a promotional brochure sent out in July of 1997 to its government customers, Information America boasts that its People Finder database contains credit header information on "160 million individuals, 92 million households, 71 million telephone numbers, and 40 million deceased records." This promotional brochure is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

19 When consumers offer this information, they generally may not realize that it may be made publicly available, transferred, or sold and then used in ways completely unconnected from the purpose for which they initially offer it.

20 Comments of IRSG at 3 (Doc. No. 35).

21 One noteworthy exception requires the Internal Revenue Service to disclose the contents of a tax return only in limited circumstances, such as in connection with conducting an income tax audit or locating the recipient of a tax refund. 26 U.S.C. § 6103 (1997). Another exception is a law prohibiting the Census Bureau from publishing information that would identify a particular individual. 13 U.S.C. § 9 (1997).

22 Lane, *supra* n. 7, at 251-79.

23 *See, e.g.*, Lane, *supra* n. 7, at 251-79.

24 *Id.*

25 About half the states restricted access to or use of voter registration records as of 1996. Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law*, Michie Law Publishers, Charlottesville, VA, 1996 at 54 (citing Robert Gellman, "Public Records: Access, Privacy and Public Policy" (1995) (unpublished)).

26 Information America recently promoted its "FAA Airmen Directory" as containing, for all individuals registered to fly in the US, "information such as pilot's name, address, FAA region, certification class, medical certificate type and date of last medical exam." This promotional brochure is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

27 Subject to its ability to withstand constitutional scrutiny, the federal Driver's Privacy Protection Act of 1994 ("DPPA"), effective as of September of 1997, may limit states' traditional practice of releasing motor vehicle records upon request. The DPPA requires that individuals be given some control over the release of their information, by limiting the circumstances under which the information can be disclosed unless "the motor vehicle department has provided in a clear and conspicuous manner on forms for issuance or renewal of operator's permits, titles, registrations, or identification cards, notice that personal information collected by the department may be disclosed to any business or person, and has provided in a clear and conspicuous manner on such forms an opportunity to prohibit such disclosures." 18 U.S.C. §§ 2721-2725 (1994). Two district courts have struck down the DPPA on Tenth Amendment grounds. *Condon v. Reno*, 972 F. Supp. 977 (D.S.C.1997), *appeal pending*; *Oklahoma v. United States*, 1997 U.S. Dist. LEXIS 14455 (W.D. Okla. 1997), *appeal pending*.

28 Twenty-two states used the Social Security number as the driver identification number as of 1994. Testimony of Congressman James P. Moran, Before the House Subcommittee on Civil and Constitutional Rights on HR 3365, The Driver's Privacy Protection Act of 1993, 2/3/94, 1994 WL 14167988 (page unavailable online). Some states allow individuals the option of not using their Social Security number. *See, e.g.*, Va. Code Ann. § 46.2-342 (1997).

29 FRB Report, *supra* n. 2, at 6.

30 The sale of digitized records is providing governments with a new revenue stream. Illinois, for example, makes $10 million a year selling public records and Rhode Island makes $9.7 million selling Department of Motor Vehicle Records ("DMV") records alone. Bernstein, *supra* n. 15, at 1.

31 Transcript, Wenger at 109.

32 *Id.*

33 Comments of IRSG at 5 (Doc. No. 35).

34 Transcript, Hogan at 105-07; Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

35 Lane, *supra* n. 7, at 130-31; Comments of IRSG at 6 (Doc. No. 35); Transcript, Hanna at 129

36 *See, e.g.*, Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

37 *See* Lane, *supra* n. 6, at 57-59; Transcript, Lane at 48-50.

38 Transcript, Lane at 51-52.

39 For example, an information supplier could solicit information from individuals for the precise purpose of enabling them to be found through a look-up service. Some self-reported information, such as information voluntarily posted on one's own Web site, may be publicly available as well.

40 *See* Transcript, Ford at 112.

41 Equifax does not sell credit header information to private investigators and its locator products do not contain Social Security numbers. Transcript, Ford at 113-14.

42 The FCRA allows credit reports to be distributed only to entities with specified "permissible purposes" (such as evaluating individuals for credit, insurance, employment, or similar purposes) under specified conditions (such as certification from the user), and provides for certain consumer rights in connection with the information maintained by credit reporting agencies (*see infra* n. 84). 15 U.S.C. §§ 1681-1681u (1997). A consumer reporting agency may not furnish medical information in connection with employment, credit, insurance, or direct marketing without the consent of the consumer. Section 604(g), FCRA, 15 U.S.C. §§ 1681b (1997).

43 Comments of the DMA at 1(a) (Doc. No. 14). The DMA's Guidelines for Personal Information Protection indicate that personal information collected for marketing "should only be used" for marketing purposes and the DMA maintains that its Committee on Ethical Business Practice reviews complaints regarding the alleged use of marketing data for non-marketing purposes. Comment of the DMA at 1(b) (Doc. No. 14). Further, a Senior Vice President of the DMA has stated explicitly that magazine subscription lists and direct marketing lists may not be used by individual reference services. Transcript, Cerasale at 74. *See also* Transcript, Quarles at 238-39 (representing that Metromail's marketing information was not available to look-up services).

44 For example, the Web sites of several online individual reference services represent that information in their databases originates from subscription and marketing lists. *See, e.g., DigDirt, Inc.* (visited on November 26, 1997) <http://www.pimall.com/digdirt/mo00008.html>; *The Cat Midwest* (visited November 26, 1997) <http://visi.com/thecat/missing1.html#seal>; *DocuSearch*, (visited on November 26, 1997) <http://www.docusearch.com/search_descriptions.html#locate>. *See also* Transcript, Lane at 47, 50-51 (stating that the some unlisted phone numbers can be accessed through the Internet because database operators purchase marketing lists, and these lists are increasingly being merged with other databases). During the Workshop, representatives of individual reference services, both online and offline, appeared unsure as to whether their databases incorporated information from direct mail and magazine subscription lists. *See* Transcript, Reed at 71-73 (stating that information products obtained from Metromail and sold by IRSC, an offline reference service (*i.e.*, a service not operating over the Internet), originated from direct mail and magazine subscription lists); Reed at 245 (retracting his earlier statement, and stating that he had been informed that Metromail has not sold information obtained from marketing transactions since 1994); Hanna at 76-77 (admitting that he did not know the current source of information products obtained from Metromail and First Data Corporation and sold by WDIA, an online reference service, but asserting that at least in the past they had originated from marketing information). At least one information vendor, Metromail, once allowed individual reference services to access such marketing databases in real-time to retrieve information for their customers. *See* Transcript, Reed at 71-73; Transcript, Hanna at 76-77.

However, Metromail maintains that it stopped providing marketing information to look-up services in 1994. Transcript, Medine, Quarles, Reed at 244-45. This past year CDB Infotek, another service, advertised a "skip tracing" tool containing "over 12 million address changes reported to national magazine publishers." *CDB Infotek* (visited March 28, 1997) <http://www.cdb.com/public/services/locate.shtml> This type of promotional material triggered a well-publicized complaint to the DMA against CDB Infotek in April of 1997. *See, e.g.*, "A Moment of Truth, Self-Regulation, How it Really Works," *DM News*, page 44, April 21, 1997. Now, however, this service's Web site makes no mention of such a tool. *CDB Infotek* (visited November 26, 1997) <http://www.cdb.com/public>

45 *E.g., DigDirt, Inc.* (visited November 26, 1997) <http://www.pimall.com/digdirt> (travel records and phone records); *The Cat* (visited November 26, 1997) <http://www.visi.com/thecat/missing1.html#sea1> (utility records).

46 For example, one individual reference service combines information from telephone directories and public records. Comments of LEXIS-NEXIS at 2 (Doc. No. 18).

47 Comments of IIA (Doc. No. 32) at 18.

48 Transcript, Reed at 74. To the extent an individual reference service provides customers with consumer reports (containing, *e.g.*, credit history, financial status, and employment background information), that entity may be acting as a "consumer reporting agency" subject to the obligations and restrictions set forth in the FCRA.

49 *E.g.*, Comments of Biggerstaff at 4 (Doc. No. 3); Comments of Privacy Rights Clearinghouse ("PRC") at 1 (Doc. No. 6). As these types of information become more widely available, they may become less useful as unique identifiers, and society may have to begin using other identifiers. Some under development include digital key signatures and biometrics such as retinal scans and digitized fingerprints. *See, e.g.*, Comments of Electronic Information Privacy Center ("EPIC") at 7 (Doc. No. 26).

50 For example, at one time, one information provider, Metromail, provided access to the names, home addresses, and ages of children over a 900 number for three dollars a minute. This service has since been discontinued. Comments of EPIC at 6 (Doc. No. 26). In fact, Metromail along with certain other services, like LEXIS-NEXIS, have discontinued making available for wide commercial distribution non-public records about minors. Comments of IRSG at 12 (Doc. No. 35).

51 *DigDirt Inc.* (visited on November 26, 1997) <http://www.pimall.com/digdirt/mo00016.htm>. Commission staff has not verified the accuracy of these representations.

52 As discussed in more detail below, customers may have to pay subscription and monthly fees in addition to the costs of individual searches. *See* discussion at n. 59 *infra* and accompanying text.

53 Typically, searches accessing higher numbers of databases that contain larger amounts of records cost more, as do searches for harder-to-obtain pieces of information.

54 Although online commercial providers may not charge consumers directly for accessing information, they may otherwise profit from making the information available, such as through advertisements on their Web sites.

55 For an in-depth discussion of which public records are available online, *see* Lane, *supra* n. 7, ch. 31.

56 Comments of IRSG at 10 (Doc. No. 35) (discussing the practices of eight individual reference services).

57 *See, e.g.*, Comments of LEXIS-NEXIS at 3 (Doc. No. 18).

58 Comments of CDB Infotek at 4 (Doc. No. 20); Comments of IRSG at 11 (Doc. No. 35) (discussing the practices of Database Technologies); Transcript, Hogan at 107-08.

59 Comments of IIA, Appendix at 18 et. seq. (not paginated) (Doc. No. 32). One service, for example, charges an initiation fee of $130, a monthly fee of $30, and per-search charges ranging from $7 to $32. *Id.*

60 Transcript, Hogan at 107-09; Abrams at 128.

61 Notwithstanding the Commission's request for information, few companies volunteered specific information about their access limitations, contractual use limitations, or prices, presumably due to proprietary concerns.

62 Comments of IIA at 22 (Doc. No. 32); Comments of IRSG at 11 (Doc. No. 35); Comments of NCISS at 3 (Doc. No. 11).

63 Experian, for example, requires a nexus between the end user and the data subject when providing current and past addresses and Social Security numbers to organizations that use the information to locate or authenticate individuals. Transcript, Abrams at 114-15. For example, an insurance company would have a sufficient nexus to an uninsured individual who caused a car accident involving a motorist insured by the company. *Id.* at 116.

64 Comments of IIA at 22 (Doc. No. 32); Comments of NCISS at 3 (Doc. No. 11); Transcript, Hogan at 107. For example, each of the four databases to which the National White Collar Crime Center subscribes examined the center's operation before granting it a subscription. However, the look-up services have not conducted any formal audits of the center's uses. Transcript, Belcher at 148-49.

65 Comments of IIA at 22 (Doc. No. 32).

66 Comments of IIA at 22-23 (Doc. No. 32).

67 Comments of IRSG at 12 (Doc. No. 35). LEXIS-NEXIS' P-Trak database, for example, does not display Social Security numbers. Transcript, Welch at 21. Other services display Social Security number only on a truncated basis, *i.e.*, by replacing the last four digits with X's. Transcript, Hanna at 41. A customer, however, may use a Social Security number as a search term if she already knows that number. Transcript, Welch at 21; Hanna at 40-41.

68 Comments of IRSG at 12 (Doc. No. 35) (discussing the practice of LEXIS-NEXIS, Metromail, and other services, which avoid making available non-public information about minors, and the practice of Database Technologies and IRSC, which make such information available only for limited purposes, for example to search for missing children); Transcript, Welch at 22 (noting that LEXIS-NEXIS' P-Trak and P-Find databases do not contain information about individuals identified as being under the age of 18).

69 Comments of IRSG at 12 (Doc. No. 35) (discussing, for example, LEXIS-NEXIS' practice of displaying an on-screen notice describing uses of the information that are covered by the FCRA).

70 Transcript, Reed at 123; Abrams at 128.

71 Comments of NCISS at 4 (Doc. No. 11); Comments of IRSG at 11 (Doc. No. 35) (discussing the practices of Database Technologies).

72 Transcript, Dick at 59-60. A newspaper article reports that according to Jack Reed, president of an individual reference service and of NCISS, roughly 200 legitimate resellers of identifying information have sprung up on the Internet. Ed Mendel, "What Others Know Can Hurt You, *San Diego Union Tribune*, May 15, 1997 at A1. Privacy

advocate Beth Givens, states that she finds a new online service everyday. Transcript, Givens at 189. Carole Lane, author of *Naked in Cyberspace*, estimates that the number of online individual reference services, if broadly defined, would be in the thousands. Transcript, Lane at 190.

73 *See, e.g.*,Transcript, Hanna at 37 (discussing service available to general public over Internet through WDIA) and Lane at 44-47 (discussing services available to general public over Internet).

74 DBT-Online reportedly offers this service to its 20,000 customers. Bernstein, *supra* n. 15, at 1.

75 Comments of IRSG at 10 (Doc. No. 35) (discussing the practices of eight individual reference services).

76 Transcript, Hanna at 38.

77 *See, e.g.*,Transcript, Lane at 46 (discussing a service made available over the Internet only to subscribers of CDB Infotek).

78 Transcript, Dick at 301.

79 *Id.* at 60.

80 *E.g.*, Transcript, Panzera at 138; Belcher at 146; Baity at 158-59; Comments of the National Council of Investigation and Security Services ("NCISS") at 3 (Doc. No. 11); Comments of Archer at 2 (Doc. No. 22).

81 *See, e.g.*, Transcript, Belcher at 146; Comments of IRSG at 1 (Doc. No. 36). "Twenty percent of the population change address on an annual basis." Transcript, Abrams at 235

82 Transcript, various participants at 136-60. For example, one service reports that the following entities subscribe to its services: FBI, IRS, Health Care Financing Administration, and the US Department of Justice. Comments of CDB Infotek at 1 (Doc. No. 20).

83 *E.g.*, Comments of USSS at 1 (Doc No. 28); Comments of National White Collar Crime Center ("White Collar Crime Center") at 1 (Doc. No. 33); Transcript, Panzera at 137-38; Belcher at 144-45; Baity at 158-59.

84 Transcript, Baity at 158-59; Belcher at 154-55; Panzera at 137-38

85 Comments of White Collar Crime Center at 1 (Doc. No. 33).

86 Transcript, Panzera at 137-38; Comments of USSS at 1 (Doc. No. 28).

87 Comments of White Collar Crime Center at 1 (Doc. No. 33).

88 *See FinCEN* (visited on December 5, 1997) <http://www.ustreas.gov/treasury/bureaus/fincen/faqs>; Transcript, Baity at 158.

89 Transcript, Baity at 156-57. In addition to its financial database, FinCEN uses roughly fifteen commercial databases, and has access to almost all law enforcement databases. *Id.*

90 In fact, FinCEN's analysts provide case support to more than 150 federal, state, and local agencies and issue approximately 8,000 intelligence reports each year. *FinCEN* (visited December 5, 1997) <http://www.ustreas.gov/treasury/bureaus/fincen/faqs>.

91 Transcript, Baity at 157.

92 *Id.*

93 Comments of White Collar Crime Center at 1 (Doc. No. 33); Transcript, Belcher at 147.

94 Contrary to the assertions of the individual reference services, some industry critics maintain that another private sector use -- marketing -- is what actually drives the industry. *E.g.*, Transcript, Sobel at 214. Again, databases used primarily for marketing fall outside the scope of this study.

95 *See* Comments of IRSG at 13-15 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Transcript, J. Byrne at 207 (bank industry representative noting that the Secret Service is "great at investigating credit card fraud but that they can't do everything"); Transcript, Hulme at 228 (representative of NCISS asserting that the private security sector is twice as large as the public security sector); Transcript, Jensen at 165-66 (representative of a non-governmental child support enforcement agency asserting that without the help of agencies like theirs, custodial parents in dire financial straits could have to wait a long time for services to be rendered by their government counterparts, and potentially jeopardize their children's health and safety); Comments filed by individual members of the private investigation and information industry (Doc. Nos. 39-243, 245-271) [hereinafter "Comments of Private Investigation Industry"] (stating that the free flow of information allows the public, who would otherwise not have the resources, to defend themselves without relying on government for help).

96 *See* Comments of IRSG at 13-14 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (*e.g.*, Doc. Nos. 43, 47, 67, 78, 103, 141, 143, 149, 182, 197, 206); Transcript, J. Byrne at 207; Transcript, Jensen at 165-66.

97 Comments of CDB Infotek at 2 (Doc. No. 20); Comments of IRSG at 14 (Doc. No. 35).

98 *See* Transcript, Reed at 121-22.

99 Comments of National Retail Federation ("NRF") at 5 (not paginated) (Doc. No. 21); Transcript, Duncan at 205-07; Comments of GE Capital at 1 (not paginated) (Doc. No. 2); Comments of IRSG at 14 (Doc. No. 35).

100 Comments of NRF at 5 (not paginated) (Doc. No. 21); Transcript, Duncan at 205-07; Comments of IRSG at 14 (Doc. No. 35).

101 Comments of American Bankers Association ("ABA") at 2-3 (Doc. No. 1); Transcript, J. Byrne at 207-08.

102 Comments of ABA at 3 (Doc. No. 1).

103 *Id.*

104 *Id.*

105 Due diligence refers to a legal requirement compelling individuals to diligently verify certain information before taking various types of actions, *e.g.*, verifying the financial status of an entity before a merger or acquisition.

106 Comments of IRSG at 9, 15 (Doc. No. 35).

107 Transcript, Duncan at 206 (noting that credit grantors in retail industry use services in deciding whether to grant credit); Comments of ABA at 3 (Doc. No. 1) (noting that banks use services to ensure that potential bank employees have clean criminal records); Transcript, Reed at 195-96 (noting that the corporations use credit header

information to detect misrepresentations on job applications); Transcript, Sobel at 214 (asserting that services are used to make employment, insurance, and credit decisions); Transcript, Givens at 182-84 (asserting that services are used to make employment decisions).

108 Workshop participants and entities that submitted comments to the Commission were not clear as to whether credit and employment decisions are based on consumer reports (containing, *e.g.*, credit history, financial status, and employment background information). *See, e.g.*, Transcript, Duncan at 206 (retail industry representative referring to the information obtained from database services as a "credit report"); Comments of Independents Bankers Association of America ("IBAA") at 4-5 (not paginated) (Doc. No. 24) (bank association referring to individual reference services, including LEXIS-NEXIS, as "credit bureaus"); Transcript, Sobel at 214 (asserting that services are used to make employment, insurance, and credit decisions); Transcript, Givens at 182-84 (stating that services are used to perform background checks on potential employees). This lack of clarity likely stems from the fact that certain individual reference services also act as credit bureaus. Transcript, Hanna at 39-41; Reed at 194. Such services, in addition to providing basic identifying information, also provide consumer reports pursuant to the requirements set forth in the FCRA. Transcript, Hanna at 39-41; Reed at 194.

109 Under the FCRA, in such situations data subjects about whom adverse decisions are made are entitled, *inter alia*, to receive an adverse action notice stating the name, address, and phone number of the consumer reporting agency that provided the data leading to the action (Section 615, 15 U.S.C. § 1681m (1997)), to obtain all the information in the agency's file on them (Section 609, 15 U.S.C. § 1681g (1997)), and to dispute the accuracy or completeness of the information with the agency (Section 611, 15 U.S.C. § 1681i (1997)).

110 *E.g.*, Comments of IRSG at 9 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105); Comments of LEXIS-NEXIS at 6 (Doc. No. 18).

111 Comments of LEXIS-NEXIS at 6 (Doc. No. 18).

112 Comments of CDB Infotek at 2 (Doc. No. 20).

113 *E.g.*, Comments of IRSG at 9 (Doc. No. 35); Comments of CDB Infotek at 2 (Doc. No. 20); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105).

114 *E.g.*, Comments of IRSG at 9, 17-18 (Doc. No. 35); Comments of CDB Infotek at 2-3 (Doc. No. 20); Comments of LEXIS-NEXIS at 5 (Doc. No. 18); Comments of NCISS at 2 (Doc. No. 11); Comments of Private Investigation Industry (Doc. No. 105).

115 *E.g.*, Comments of NCISS at 2 (Doc. No. 11); Comments of IRSG at 13-19 (Doc. No. 35); Comments of Private Investigation Industry (Doc. No. 105).

116 *See* Comments of NCISS at 2 (Doc. No. 11); Comments of IRSG at 15-19 (Doc. No. 35); Comments of Private Investigation Industry (Doc. No. 105).

117 *See* Comments of IRSG at 15-19 (Doc. No. 35); Comments of NCISS at 2 (Doc. No. 11).

118 Comments of LEXIS-NEXIS at 6; Transcript, Edington at 221-22; Comments of IRSG at 19-20 (Doc. No. 35).

119 Transcript, Hulme at 229; Allen at 317-18; Comments of Child Quest International at 1(Doc. No. 106).

120 Comments of Childcare Checkpoint (Doc. No. 34).

121 Comments of IRSG at 19 (Doc. No. 35).

122 Transcript, Jensen at 161-64; Comments of Association for Children for Enforcement and Support ("ACES") (not paginated) (Doc. No. 4); Comments of IRSG at 15 (Doc. No. 35). One non-profit organization relies heavily on an offline service to enable mostly low-income, single mothers to track down current addresses for absent, non-paying parents. Comments of ACES at 1 (not paginated) (Doc. No. 4).

123 *Id.* at 2. This organization states that in the past ten years it has been able to assist over 25,000 families in finding non-paying parents using some type of computerized database, which translates into families collecting an average of $4,000 per year in child support. *Id.*

124 Transcript, Jensen at 163-64.

125 Transcript, Kirtley at 169; Comments of Reporters Committee for Freedom of the Press ("Reporters Committee") at 2 (Doc. No. 16).

126 Transcript, Kirtley at 170-72; Comments of Reporters Committee at 3-4 (Doc. No. 16).

127 Transcript, Kirtley at 180.

128 Comments of IRSG at 18-19, 21 (Doc. No. 35); Comments of CDB Infotek at 3 (Doc. No. 20).

129 Transcript, Reed at 121-22.

130 Comments of IIA at 20 (Doc. No. 32).

131 Comments of Junkbusters at 11 (Doc. No. 15).

132 One potential means would be to sue a look-up service that provided inaccurate information on grounds of libel. However, such actions lie only if there is injury to a data subjects's reputation. Comments of Reporters Committee at 4 (Doc. No. 16). Furthermore, only in rare circumstances would the data subject learn of the inaccuracy and have the ability to trace it back to the look-up service.

133 Survey results form 1978 to 1994 indicate that increasing numbers of consumers have expressed concern about threats to their personal privacy in America. Louis Harris and Associates, Inc., *Interactive Services, Consumers and Privacy* (conducted for *Privacy and American Business*) (1994) [hereinafter "1994 Harris Survey"] at 1; Louis Harris & Associates 1996 *Equifax-Harris Consumer Privacy Survey* (conducted for Equifax, Inc.) (1996) [hereinafter "1996 Harris Survey"]. In fact, in late 1996, this figure rose to 89%. *Hearing on "Electronic Payment Systems, Electronic Commerce, and Consumer Privacy Before the Subcomm. on Financial Institutions and Consumer Credit, House Comm. on Banking and Financial Services*, Sept. 18, 1997 (Statement of Dr. Alan F. Westin) [hereinafter "Westin Testimony"]. Yet another survey demonstrates that 80% of Americans feel that "[c]onsumers have lost control over how personal information about them is collected and used by companies." 1997 Harris Survey at xvii (reporting that 80% of computer users in 1997 and that 80% of all Americans in 1995 agreed with this statement). Survey research also indicates that people differ in their conception of privacy -- roughly 25% are "privacy fundamentalists" and do not want to disclose personal information in return for opportunities and benefits; about 20% have little or no concern and willingly disclose their information; and the majority evaluate their privacy concerns on a case-by-case basis. Westin Testimony; Federal Trade Commission's Bureau of Consumer Protection, *Staff Report*, "Public Workshop on Consumer Privacy on the Global Information Infrastructure," (December 1996) [hereinafter "FTC 1996 Privacy Report"] at n. 25 and accompanying text (citing Westin). The individuals who decide on a case-by-case basis consider the following types of factors: the nature of the benefit being offered in exchange for personal information; what potential misuses of this information can be

made; and whether adequate safeguards are in place to protect their information. *Id.* For an in-depth discussion of laws recognizing information privacy interests, see generally Schwartz & Reidenberg, *supra* n. 25.

134 A.R. Dowd, "Protect Your Privacy," *Money Magazine*, Aug. 1997 at 107.

135 *See, e.g.*, Transcript, Givens at 181-82; Grant at 197; Comments of Privacy Rights Clearinghouse ("PRC") at 1 (not paginated) (Doc. No. 6); Comments of EPIC at 11 (Doc. No. 26); Comments of CDT at 6 (Doc. No. 29).

136 *See* n. 1, *supra* and accompanying text; Comments of EPIC at 6 (Doc. No. 26); Comments of PRC at 1 (not paginated) (Doc. No. 6); Comments of CDT at 6 (Doc. No. 29).

137 *See* Transcript, Hendricks at 321; L. Byrne at 211; Comments of EPIC at 8 (Doc. No. 26); Comments of PRC at 2 (not paginated) (Doc. No. 6); Lane, *supra* n. 7, at 45.

138 Comments of EPIC at 8 (Doc. No. 26); *see also* Transcript, Berman at 91.

139 Consumers whose information in the databases enables them to claim an inheritance or collect a judgment do directly benefit from the services, as may consumers whose database information allows them to be found by a long-lost relative or friend. Some consumers, however, may prefer not to be found at all.

140 *See* Comments of PRC at 2 (not paginated) (Doc. No. 6); Comments of EPIC at 11 (Doc. No. 26); Comments of National Consumers League ("NCL") at 3 (Doc. No. 12). One notable exception is LEXIS-NEXIS, which allows consumers to opt out of its P-Trak database. Transcript, Glass at 67. Furthermore, LEXIS-NEXIS is now planning to allow consumers to access their identifying information maintained in its P-Trak and P-Find databases. Comments of LEXIS-NEXIS at 2 (Doc. No. 18A). These databases are two of the 7,000 databases that LEXIS-NEXIS maintains. Transcript, Welch at 19.

141 *E.g.*, Comments of Avrahami at 1 (Doc. No. 23); Comments of CDT at 3 (Doc. No. 29); Comments of EPIC at 7 (Doc. No. 26); Comments of Junkbusters at 7 (Doc. No. 15); Transcript, Wenger at 86; Grant at 198; Sarna at 309-10. *See also* 1996 FTC Privacy Report at n. 24 and accompanying text.

142 Similarly, a significant number of Americans choose not to make their phone numbers publicly available. In 1996, 33% of Americans were reported to have unlisted phone numbers. Schwartz & Reidenberg *supra* n. 25 at 243.

143 People tend to perceive comprehensive data profiles as more intrusive than disparate bits of information. Smith, *supra* n. 7, at 7-9.

144 Comments of Biggerstaff at 6 (Doc. No. 3).

145 *E.g.*, Transcript, Sarna at 310; Comments of Junkbusters at 7 (Doc. No. 15).

146 Comments of CDT at 3-4 (Doc. No. 29); Transcript, Dick. In fact in a recent survey, 28% of consumers said they refuse to disclose their income range for marketing purposes. B. Negus, "You're Not Welcome," *Direct Magazine*, June 15, 1996 at 61, 63-64. Again, services used primarily for marketing are beyond the scope of this study.

147 *E.g.*, Comments of Biggerstaff at 7 (Doc. No. 3).

148 Transcript, Rotenberg at 88. This shift in comfort level was demonstrated when the Social Security Administration, in response to a deluge of complaints, withdrew its service of providing consumers with their files

over the Internet within three days of initiating the service. Transcript, Hendricks at 84, Rotenberg at 88. The Social Security Administration has since resumed this Internet service, providing less information than before, with more privacy and security protections in place. *Social Security Administration* (visited December 8, 1997) <http://www.ssa.gov>.

149 *E.g.* Comments of CDT at 3-4 (Doc. No. 29).

150 The public response to LEXIS-NEXIS making Social Security numbers available through P-TRAK is discussed at n. 1 *supra*. As mentioned above, a recent *Money Magazine* poll indicates that 88 % of respondents are concerned about the sale of their Social Security number and other sensitive identifiers. A.R. Dowd, *supra* n. 134, at 107. The 1994 Harris Survey found that over 60% of the population was concerned that their Social Security number would be misused in the future. Yet, another survey found that over 95% of the public object to the collection of their Social Security number for marketing purposes. Negus, *supra* n. 146, at 61, 63-4. At the same time, however, consumers provide their Social Security numbers in many marketing transactions where this number is requested but likely not necessary, *e.g.*, in applying for membership at a video rental store.

One survey has found that consumers also object to marketers collecting the following types of information: age (44%); approximate annual income (81%); length of time spent living at current address (46%); names and ages of children in the household (77%); height and weight (62%); spending limit on credit cards (90%). Negus, *supra* n. 146, at 61, 63-4.

151 *See* Comments of EPIC at 8 (Doc. No. 26); Comments of Biggerstaff at 6 (Doc. No. 3); Transcript, Sarna at 310; Sobel at 216-18; Comments of IBAA at 3 (not paginated) (Doc. No. 21). These risks are discussed further at Section IV.C. *infra*.

152 Comments of Biggerstaff at 6 (Doc. No. 3).

153 *See, e.g.*, Transcript, Sarna at 310.

154 Public Opinion Strategies, *A Telephone Survey of Adults in the Continental United States* (conducted for the National Association to Protect Individual Rights) (1993) at 4.

155 1997 Harris Survey at xviii.

156 1996 Harris Survey at 40.

157 *Id.*

158 *Id.*

159 These examples are not as far-fetched as they may appear; the latter two are loosely based on complaints the Commission has received in the credit reporting area.

160 *See* discussion at n. 107 and 109 *supra* and accompanying text.

161 United States Government, National Information Infrastructure Task Force, Information Policy Committee, *Options for Promoting Privacy on the National Information Infrastructure*, Draft for Public Comment (1997) at 6.

162 Transcript, Reed at 71; Lane, *supra* n. 7, at 53.

163 Some LEXIS-NEXIS products, for example, display the following warning: "This data is compiled by a third party from multiple sources. INACCURACIES DO EXIST." (emphasis in original).

164 Transcript, Hogan at 106.

165 Comment of IIA at 21-22 (Doc. No. 32).

166 *E.g.*, Comment of IIA at 23 (Doc. No. 32); Transcript, Tobin at 274; Comments of Private Investigation Industry (*e.g.*, Doc. Nos. 42, 46-49, 51, 53, 55, 56, 58-64, 66-69).

167 Lane, *supra* n. 7, at 53.

168 *Id.* at 252.

169 *Id.* at 53, 252. For example, a file may be out of place during the scanning process. *Id.* at 252.

170 *See* Lane, *supra* n. 7, at 53. Harm from mismatched files can be devastating. For example, in a situation that involved a computerized database, although not necessarily a look-up service, a New York man was targeted for skipping child support payments to a son he did not have. Public Advocate for New York City, Annual Report (1997) at 5. After his wages and income tax refunds were withheld, a warrant was put out for arrest, and he was fired from his job, the man discovered that the child welfare authorities had confused his record with that of an individual with the same name who did owe child support. *Id.* The Computer Matching and Privacy Protection Act regulates the compilation of data from automated record systems (data matching) by the federal government. It addresses potential problems posed by the compilation of data. This act requires, *inter alia*, that federal agencies independently verify matched data before taking adverse action regarding data subjects and give data subjects the opportunity to challenge the data's accuracy, unless only certain limited information is relied on for certain purposes. 5 U.S.C. § 552a(p) (1997).

171 *E.g.*, Transcript, Reed at 123-24; Comments of Junkbusters at 20 (Doc. No. 15); Comments of EPIC at 11 (Doc. No. 26); Comments of Biggerstaff at 20 (Doc. No. 3); Comments of PRC at 2 (not paginated) (Doc. No. 6).

172 Transcript, Glass at 68.

173 Transcript, L. Byrne at 211.

174 When an adverse action is based on information from a consumer report, the FCRA requires the *user* to provide the consumer with a notice that sets forth (1) the fact that adverse action has been taken in whole or part based on information contained in a consumer report; (2) the name, address, and phone number of the consumer reporting agency that provided the report; (3) a statement that the agency did not make the decision and can not provide the specific reasons for the adverse action; and (4) a notice of the rights provided consumers by the FCRA to (A) obtain a free copy of their credit file upon request within 60 days, and (B) dispute information in their file they believe is inaccurate or incomplete. FCRA, § 615, 15 U.S.C. § 1681m (1997). Furthermore, when credit is denied or the charge for credit increased based on information *bearing on a consumer's credit worthiness* from any source *other than a consumer reporting agency* (*e.g.*, from a reference on a loan application or from information obtained through an individual reference service), section 615(b) requires that users, upon request, disclose to the consumer the nature of that information. FCRA, § 615(b), 15 U.S.C. § 1681m (1997). This is a more limited disclosure than the FCRA provides to a consumer who suffers adverse action based on a consumer report.

The Commission has brought actions against employers and creditors for failure to give consumers adverse action notices pursuant to Section 615 in the absence of consumer complaints, finding that wronged consumers have no way of knowing about such violations, and therefore would never know to complain. *See In re*

Aldi Inc., FTC Docket No. C- 3764 (1997); *In re Brunos, Inc.* FTC Docket No. C-3760 (1997); *FTC v. Bonlar Corp*, Inc., 97-C-7274 (N.D. Ill. 1997); *In re Electronic Data Systems Corp.*, FTC Docket No. C-3342 (1991); *In re Keystone Carbon Company*, FTC Docket No. C-3360 (1992); *In re The Kobacker Co.*, FTC Docket No. C-3359 (1992); *In re Macy's Northeast, Inc.*, FTC Docket No. C-3362 (1992); *In re McDonnell Douglas Corporation*, FTC Docket No. C-3361 (1992).

175 A computer hacker is an individual who wrongfully gains access to computerized data through technological means.

176 In other cases, individuals who access the services for apparently legitimate reasons may use the information for what could be perceived as offensive, if not unlawful, purposes. Private investigators, for example, who access the services may engage in "pretexting," *i.e.*, using information to pose as the data subject and thereby probe more deeply into that individual's affairs, *e.g.*, to obtain an itemized telephone or credit card bill. Journalists may use the services to unearth and disseminate embarrassing facts about celebrities. An employer may use the databases to find answers he was not allowed to ask during a job interview, including age and marital status. A lawyer may comb through a service's databases looking for potentially damaging information, unrelated to the case at hand, about opponents or their lawyers, in the hope of using the information to dissuade them from going forward with the case. (In fact, this very practice was alleged by individuals who had been harmed by an explosion at a Texaco oil refinery in a suit against Texaco and its agents. Bernstein, *supra* n. 15, at 1.) Finally, voyeuristic individuals may inquire into their neighbors' and coworkers' records for their own amusement.

177 Comments of the Cuneo Law Group (Doc. No. 244). The prison had been subcontracted to do data entry in connection with a project for a prominent information vendor. *Id.*

178 D. Szwak, "Theft of Identity: Data Rape," *Michigan Bar Journal*, March 1995; Comments of NCL at 2 (Doc. No. 12).

179 J.K. Bloom, " Alleged Spree Highlights Danger of Identify Theft," *The American Banker*, June 3, 1997 at 1.

180 Comments of NCL at 2 (Doc. No. 12); Comments of WorldPages at 6 (not paginated) (Doc. No. 271). A firewall is a combination of hardware and software that separates a local area network (LAN) into two or more parts, restricting outsiders to the area "outside" the firewall while protecting the information that is maintained "inside" the firewall.

181 Comments of Junkbusters at 21 (Doc. No. 15); Transcript, Charney at 314.

182 *See, e.g.*, Transcript, Charney at 314. Even the Central Intelligence Agency's Web site proved to be vulnerable to a group of Swedish hackers. Transcript, Cattlet at 231.

183 S. Singer, "Internet Opens Your Windows to Everyone: Invasion Sorely Tests Right to Be Let Alone," *Sun-Sentinel*, August 3, 1997 ("Local" Section) at 1A.

184 B. Ward, "Online Identity Theft Crime's 'Growth Industry'," *The Ottawa Citizen*, September 15, 1997.

185 Commission staff spoke to an agent at the FBI's C-Tech (computer technology) division who stated that the Computer Emergency Response Team, based out of Carnegie Mellon University, reported 406 incidents of wrongful access to information stored in computers in 1991; 773 in 1992; 1,334 in 1993; 2,342 in 1994; 2,412 in 1995; and 2,573 in 1996.

186 Private communication from an agent at the FBI's C-Tech division.

187 Transcript, Sobel at 214; Comments of PRC at 2-3 (not paginated) (Doc. No. 6); Comments of EPIC at 8 (Doc. No. 26); Comments of NYAG at 3-4 (Doc. No. 8); Comments of CDT at 5 (Doc. No. 29); *see* also Transcript of the FTC Meeting on Identity Theft held on Aug. 20, 1996 [hereinafter "FTC ID Theft Transcript"], on file at the FTC and available over the Internet at *Federal Trade Commission, Conferences* (last updated October 1, 1997) <http:/ www.ftc.gov/ftc/conferences.htm>. The FRB found that "fraud related to identity theft appears to be a growing risk for consumers and financial institutions, and the relatively easy access to personal information may expand the risk." FRB Report, *supra* n. 2, at 21. Identity theft is a crime in which an individual impersonates her victim, using the victim's identifying information, namely the victim's name, birth date, Social Security number, driver's license number, etc. Once the thief has the name and the Social Security number, she can easily obtain any other information she needs. *See, e.g.*, FTC ID Theft Transcript; Comments of PRC at 3 (not paginated) (Doc. No. 6). The imposter assumes the new identity and uses it to run up huge credit card bills, take out loans and mortgages, and kite checks between various fraudulent bank accounts, all backed by the victim's good name.

188 Consumer liability associated with use of stolen credit cards is generally limited to $50. Truth in Lending Act, Section 133(b); 15 U.S.C. § 1643 (1997).

189 Transcript, L. Byrne at 211.

190 *See* Comments of MasterCard/Visa at 4 (Doc. No. 19); Comments of IRSG at 23 (Doc. No. 35); Comments of LEXIS-NEXIS at 7 (Doc. No. 18).

191 *U.S. v. Roger Cullen and Cheryl Cullen*, CR-97-56 (D. Del. 1997); Private communication from State of Delaware detective who investigated the case and arrested the defendants; Bloom, *supra* n. 179, at 1.

192 Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

193 Bloom, *supra* n. 179, at 1; Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

194 Private communication from State of Delaware detective who investigated the case and arrested the defendants and from US Secret Service agent who prosecuted the criminals.

One attorney who specializes in identity theft cases informed Commission staff that many recent cases of identity theft have involved perpetrators and victims living in different parts of the country. He asserted that such evidence strongly suggests that identify thieves are beginning to exploit computerized data. Private communication from David Szwak, an identity theft attorney in Shreveport, LA.

195 *Greidinger v. Davis*, 988 F.2d 1345, 1354 (4th Cir. 1993) (cited in Schwartz and Reidenberg, *supra* n. 25 at 57 and in Comments of CDT at 5 (Doc. No. 29); *see also State ex Rel. Beacon Journal Pub. v. Akron*, 640 N.E. 2d 164, 169; 70 Ohio State 3d 605 (Ohio 1994) ("Thanks to the abundance of data bases in the private sector that include the SSNs of persons listed in their files, an intruder using an SSN can quietly discover the intimate details of a victim's personal life without the victim ever knowing of the intrusion.").

196 *See e.g.*, Transcript, Hanna at 37; Welch at 27.

197 It is not far-fetched to imagine a that a crook would be willing to invest a few hundred dollars in order gain access to a few hundred thousand (especially if the crook were charging the search to someone else's credit card in the first place).

198 Transcript, Davies at 326-27, 335; Comments of IIA at 25 (Doc. No. 32); Comments of LEXIS-NEXIS at 7 (Doc. No. 18); Comments of IRSG at 21-24 (Doc. No. 35).

199 FRB Report, *supra* n. 2, at 21.

200 *See* Comments of White Collar Crime Center at 2 (Doc. No. 33); Comments of IRSG at 21-24 (Doc. No. 35). Comments of LEXIS-NEXIS at 8 (Doc. No. 18). For an example of how this fraud detection takes place, see section III.B. *supra*.

201 According to a *Money Magazine* poll, 21% of 35-44 year olds polled who had experienced an invasion in privacy later experienced stalking or other physical harassment. Dowd, *supra* n. 134, at 107; *see also* Comments of PRC at 3 (not paginated) (Doc. No. 6).

202 Comments of PRC at 3 (not paginated) (Doc. No. 6).

203 The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168055 (page unavailable online) (Statement of Donald L. Cahill, Legislative Chairman, Fraternal Order of Police). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

204 The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168013 (page unavailable online) (Statement of David Beatty, Director of Public Affairs, National Victim Center). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

205 Certain companies have stopped making available information that identifies individuals as minors. Comments of IRSG at 12 (Doc. No. 35); *see supra* n. 50

206 The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168013 (page unavailable online) (Statement of David Beatty, Director of Public Affairs, National Victim Center). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No P974806.

207 Comments of PRC at 3 (not paginated) (Doc No. 6).

208 The Driver's Privacy Protection Act: Hearings on HR 3365 Before the House Subcomm. on Civil and Constitutional Rights, February 3, 1994, 1994 WL 14168055 (page unavailable online) (Statement of Donald L. Cahill, Legislative Chairman, Fraternal Order of Police). This testimony is on file at the Federal Trade Commission's Public Reference Room, File No. P974806.

209 *See generally* Comments of New York State Dept. of Law ("NYAG") (Doc. No. 8); Comments of CDT (Doc. No. 29); Comments of Biggerstaff (Doc. No. 3); Comments of EPIC (Doc. No. 26); Transcript, Sobel at 213-17, Givens at 181-87; Sarna at 309-13; Hendricks at 320-22.

210 *See* US Dept. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (1973) [hereinafter "HEW Information Practices"], Safeguards, § I; 1996 FTC Privacy Report at 8-12; Secretary of Health and Human Services, Recommendations concerning the Confidentiality of Individually Identifiable Health Information (1997) [hereinafter "HHS Report"], § F; US Govt. Information Infrastructure Task Force, Information Policy Committee, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995) [hereinafter "IITF Principles"], § II.C.

211 *See* Section IV.A., *supra.*

212 *E.g.* Transcript, Sarna at 311.

213 *See* Transcript, Biggerstaff at 331-32; Comments of Biggerstaff at 2,12 (Doc. No. 3).

214 *See supra* n. 70 and accompanying text.

215 Journalists take the position that journalists' rights to information should be coextensive with those of the general public. Transcript, Kirtley at 174.

216 Transcript, Duncan at 205; J. Byrne at 207-08.

217 *See* Transcript, Jensen at 166-67.

218 *Id.*

219 Comments of Biggerstaff at 2 (Doc. No. 3).

220 *Id.*

221 In fact, the Privacy Act compels federal agencies to store only personal information that is relevant and necessary. 5 U.S.C. § 552a(e)(1) (1997). Certain federal laws have implemented such limitations. For example, prior to 1995, the Postal Service provided individuals' change-of-address files to any person willing to pay the $3 fee. 59 *Federal Register* 67223 (1994). Now the Postal Service restricts the availability of this information to government agencies for official purposes, to persons legally empowered to serve process, and when necessary to comply with a court order. 39 CFR 265.6(d). In deciding to amend the regulation, the Postal Service expressed concern that "no postal interest is served by furnishing the information to persons who are seeking it for reasons unrelated to the use of the mails." 59 *Federal Register* 67223 (1994). Similarly, the DPPA, discussed *supra* n. 27, limits the information states can sell, by requiring states to check for a permissible business purpose before selling motor vehicle records, unless they have provided clear and conspicuous notice to consumers and an opportunity for them to opt out of having their information sold. 18 U.S.C. §§ 2721-2725 (1994).

222 *See* Comments of IRSG at 4 (Doc. No. 35).

223 *Id.*

224 *Id.*

225 *See, e.g.*, Comments of Biggerstaff; Transcript, Sarna at 310-11. The Office of the Information and Privacy Commissioner of British Columbia is currently examining this possibility. In particular, in its study of the impact of the accessibility of real estate assessment records online, that office is considering not displaying the name of the individuals who own the property because displaying the name does not advance the purpose of enabling the public to determine the value of real estate in a particular area. Yet, not displaying the name will enable property owners to keep their home address confidential if they so choose. Remarks of Commissioner David H. Flaherty, 1997 Privacy and American Business Conference, Washington, DC October 21, 1997.

226 Transcript, Berman at 91.

227 Comments of IIA at 20-21 (Doc. No. 32).

228 *See* Comments of NCL at 2 (Doc. No. 12); Comments of CDT at 6 (Doc. No. 29); Comments of WorldPages at 6, 8 (not paginated) (Doc. No. 272).

229 *See, e.g.*, Comments of NCL at 2 (Doc. No. 12); Comments of WorldPages at 6 (not paginated) (Doc. No. 272); Comments of IBAA at 5 (not paginated) (Doc. No. 24).

230 Comments of Biggerstaff at 12 (Doc. No. 3).

231 Comments of GE Capital at 1 (not paginated) (Doc. No. 2); Comments of Biggerstaff at 12 (Doc. No. 3); *see also*, Transcript, Givens at 184; Comments of PRC at 5 (not paginated) (Doc. No. 6).

232 *See* Transcript, Givens at 184; Comments of Biggerstaff at 12 (Doc. No. 3).

233 One law enforcement representative noted that certain law enforcement functions could be undermined if audit trails were maintained and accessible. Transcript, Panzera at 143. One way to address this concern would be to keep confidential audit trails detailing uses by law enforcement.

234 *See* Comments of Junkbusters at 20 (Doc. No. 15); Comments of NCL at 3 (Doc. No. 12); Comments of CDT at 2-3 (Doc. No. 29); Comments of *Privacy Times* at 1 (not paginated) (Doc. No. 9); Comments of PRC at 5 (not paginated) (Doc. No. 6); Comments of PRC at 2 (Doc. No. 16A); Transcript, Hendricks at 321-22; Rotenberg at 325-26 ("one of the most important privacy principles there is is the right to see information about yourself held by others.").

235 *See, e.g.*, HEW Report, Safeguards § III(2); 1996 FTC Privacy Report at 8-12; IITF Principles, § III.B; HHS Report, § I.G; Privacy Act, 5 U.S.C. § 552a(d) (1997); Cable Communications Policy Act, 47 U.S.C. § 551(a)(1) (1997).

236 The FCRA allows consumers to obtain a disclosure (in writing, unless other means are requested and available) of all the information in their credit file, if they request it and properly identify themselves. FCRA, Section 609, 15 U.S.C. §1681g (1997). Consumers are entitled to this disclosure at no cost if they ask for it within 60 days of any adverse action resulting from it, and at a current fee of no more than $8.00 in any case. FCRA, Section 612, 15 U.S.C. § 1681j (1997). The FCRA further requires consumer reporting agencies to follow reasonable procedures to assure maximum possible accuracy of the information concerning an individual about whom a consumer report relates. FCRA, Section 607(b), 15 U.S.C. § 1681e (1997).

237 S. Rep. No. 517, 91st Cong., 1st Sess. 3 (1969) (legislative history to FCRA).

238 *See, e.g.*, Transcript, Grant at 201-03.

239 This is especially true when an individual is denied an opportunity because her identifying information cannot be verified, or when an individual is deprived of an earned benefit because she cannot be found.

240 Comments of IIA at 20-21 (Doc. No. 32).

241 *E.g.*, Transcript, Hendricks at 321; Comments of PRC at 3 (Doc. No. 16).

242 *See* Comments of CDT at 3 (Doc. No. 29); Transcript, Hendricks at 321-22; Comments of PRC at 5 (not paginated) (Doc. No. 6); HEW Principles, Safeguards § III(6); HHS Report, § I.G.

243 Comments of IIA at 21 (Doc. No. 32).

244 *E.g.*, Transcript, Dick at 126; Grant at 198-99; Avrahami at 306-07; Comments of CDT at 1-3 (Doc. No. 29), Comments of Junkbusters at 24 (Doc. No. 15); Comments of EPIC at 9 (Doc. No. 26); Comments of Avrahami at 2 (Doc No. 23). Some view this as the only option, because they believe that consumers are the owners of their personal identifying information. *E.g.*, Transcript, Grant at 198; Comments of Avrahami at 3 (Doc. No. 23).

245 LEXIS-NEXIS allows its customers to opt out of its P-TRAK database but not its P-FIND database. Comments of LEXIS-NEXIS at 11 (Doc. No. 18). The majority of the online white-pages directory services allow individuals to opt out of their databases. Transcript, Dick at 304.

246 Comments of EPIC at 11 (Doc. No. 26); Comments of NCL at 3 (Doc. No. 12).

247 Comments of Avrahami at 2, 8 (Doc. No. 23); Comments of EPIC at 9 (Doc. No. 26).

248 Comments of Avrahami at 8 (Doc. No. 23).

249 *E.g.*, Transcript, L. Byrne at 212-13; Avrahami at 307-08. Of course, identity theft and other types of fraud would remain as potential illegitimate economic incentives.

250 *See, e.g.*, HEW Report, Safeguards § II(3); 1996 FTC Privacy Report at 8-12; IITF Principles, § II.D.

251 *See* Transcript, Panzera at 140; Lane at 96-97; Allen at 318; Jensen at 203.

252 *See* Transcript, Baity at 160.

253 Comments of IIA at 20 (Doc. No. 32); Transcript, Panzera at 140; Lane at 96-97; Allen at 318; Jensen at 203; Comments of Private Investigation Industry (*e.g.*, Doc. Nos. 40-42, 44, 48, 50, 53-56, 58-64). Furthermore, in some cases, it makes more sense to allow consumers not to provide personal information in the first place, rather than opting out after the information has been transferred to the individual reference services, who are secondary providers

254 *See e.g.*, Transcript, Hendricks at 321-22; Comments of PRC at 3 (Doc. No. 16A); Comments of IBAA at 2 (Doc. No 24); Comments of CDT at 3 (Doc. No. 29).

255 *E.g.*, HEW Report, Safeguards § II; 1996 FTC Privacy Report at 8-12; IITF Principles, § II.B; HHS Report, § I.G.

256 *E.g.*, Transcript, Abrams at 128, 25; Rotenberg at 132; Davies at 328; Comments of NCL at 4 (Doc. No. 12); Comments of Junkbusters at 31 (Doc. No. 15); Comments of PRC at 3 (Doc. No. 16A); Comments of IBAA at 2 (Doc. No. 24); Comments of CDT at 3 (Doc. No. 29). Interactive technology is one effective means of educating consumers, as well as a tool consumers can use to raise their voices in opposition to practices they find objectionable. *See* Transcript, Berman at 92.

257 Comments of NCL at 4 (Doc. No. 12).

258 Comments of Junkbusters at 31 (Doc. No. 15).

259 *See* Transcript, Rotenberg at 132; Comments of EPIC at 15 (Doc. No. 26) (stating that the industry should be educated about legal duties, fair information practices, and new techniques to limit or eliminate the collection of personal data).

260 A copy of the "Individual Reference Services Industry Principles" is attached as Appendix D A copy of the official "Industry Principles -- Commentary" ("Commentary") is attached as Appendix E.

261 The current signatories are: Acxiom Corporation; CDB Infotek, a ChoicePoint Company; DCS Information Systems; Database Technologies, Inc.; Equifax Credit Information Services, Inc.; Experian; First Data Solutions Inc.; Information America, Inc.; IRSC, Inc.; LEXIS-NEXIS; Metromail Corporation; National Fraud Center; Online Professional Electronic Network; and Trans Union Corp

262 Principles at 1.

263 Transcript, Dick at 300-04.

264 Principle, § V. For a discussion of information obtained from non-public sources, see § II.B.3 *supra*.

265 Principles, § II.B.

266 "Appropriate," is defined as "reasonable under the circumstances reflecting a balance between the interests of individual privacy and legitimate business, governmental, and personal uses of information, including prevention of fraud." Principles at 1.

267 Principles, § V.A.

268 As discussed in note 42 *supra*, to the extent qualified subscribers have a "permissible purpose" under the FCRA, they may obtain information about an individuals' credit history, financial status, employment background, medical information, etc.

269 Principles, § X.

270 Principles, § V.B.

271 Principles, § V.C.

272 Principles, § VI.

273 Principles, §§ V.A.2; V.B.3; V.C.2.

274 Principles, § V.A.2.a.

275 Principles, §§ V.A.2.c; V.B.3.c.

276 Principles, §§ V.A.2.d; V.B.3.b.

277 Principles, §§ V.A.2.c.; V.B.3.d.

278 Principles, § IX.A. Many look-up services had not followed this practice before the Principles. Transcript, Plesser at 260.

279 Principles, § IX.B.

280 The signatories explain their refusal to provide consumers with public records information about them by stating that it would be excessively burdensome to access the numerous public records databases for every inquiry

(Commentary, App. E at 4) and that individuals can access public records that identify them at their source, the government custodian (Transcript, various participants at 265-68).

281 Principles, § II.A.

282 Principles, § III.

283 Principles, § III.A.

284 Principles, § VIII.

285 Principles, § V.C.1.

286 Principles, § VIII.

287 Principles, § I.

288 Principles, § VII.

289 Principles, §VII.

290 Principles, § XI; Commentary at 5.

291 Transcript, L. Byrne at 315-16; Allen at 316; Comments of Etrust at 4-5 (now known as TrustE) (not paginated) (Doc. No. 10); Comments of Private Investigations Industry (Doc. Nos. 39-104, 106-243, 245-271), Comments of WorldPages at 8 (not paginated) (Doc. No. 272).

292 Comments of *Privacy Times* at 1 (not paginated) (Doc. No. 9); Comments of PRC at 3 (Doc. No. 16A); Comments of NCL at 3 (Doc No. 12); Comments of EPIC at 13-14 (Doc. No. 26); Comments of Biggerstaff at 24 (Doc. No. 3); Comments of Avrahami at 8 (Doc. No. 23); Transcript, L. Byrne at 315-16; Biggerstaff at 287-89, Givens at 188; Rotenberg at 286, 324; Grant at 333; Culnan, *supra* n. 1, at 50-52. Marc Rotenberg recounted a situation in which a product, called Lotus Marketplace, containing marketing and credit information about consumers on a CD ROM was ready for release. The product, because it was a CD ROM, appeared to violate DMA self-regulatory guidelines requiring marketers to grant consumers the ability to opt out. Rotenberg claimed that the product was never released, not because DMA enforced the guidelines, but because 30,000 people complained through e-mail messages and the press. Transcript, Rotenberg at 283-86. Another example of self-regulatory guidelines not being enforced was cited by Jason Catlett, who noted a finding, reported in *DM News*, that thirty-eight percent of direct marketers were aware of fellow marketers renting house files without providing consumers notice or opt out options (a practice inconsistent with applicable self-regulatory guidelines). Transcript, Catlett at 293.

293 Transcript, Hendricks at 322; Grant at 334; Culnan, *supra* n. 1, at 50-52. A related concern is that members of a given industry may not even know about that industry's self-regulatory guidelines. Transcript, Catlett at 293 (citing a finding, reported in *DM News*, that seventeen percent of direct marketers were not aware of the DMA's systems to allow consumers to opt out from receiving mail and telephone solicitations from its members).

294 Transcript, Hendricks at 322.

295 Transcript, Sarna at 311-12; Hendricks at 319; Rotenberg at 324.